ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

Restriction of Image Retrieval for Shared Images over Social Networking Sites

S SUREKHA [1], M DINESH KUMAR [2], S.ARAVINDH [3]

[1]Pursing M.E, Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.
[2]Assistant Professor, Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.
[3]Assistant Professor, Department of Computer Science and Engineering, Gojan School of Business and Technology, Redhills, Chennai – 600052, Tamil Nadu, India.

Abstract: Nowadays, people are interested to share their images through social sites, but maintaining privacy for the images has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. Though many policies are set for images, even then the images are not secure. Sometimes the images are exposed or retrieved through various search engines. To overcome this problem, there is need of some tools to help users control access to their shared image. To deal with this issue, the paper proposed to set a signature for each newly uploaded image to site by using the image's features (size, shape and color) through discrete wavelet transformation algorithm. This technique helps users to overcome the problem of existing system.

Keywords-Social networking sites, DWT algorithm, Image's features.

1. INTRODUCTION

With the advancement in technology, communication has grown. It is now easier and cheap to communicate and connect with people across the world. The issue of distance is no longer an excuse for lack of communication. Communication systems have grown from wired devices to wireless devices. The internet has also brought adverse changes in the forms of communications that are available and currently being used. It has led the rise of social networks. It is easy to share information like pictures, advertisements, videos and text messages. To many people, it is perceived as a form of entertainment. However, being in social sites enhances communication.

Social networks allow people to keep and manage accounts. This is an identity and you can custom it depending on how your target group knows you. This makes it easy for individuals to search for you and get you. You also have a choice to invite people to your account. This makes it easy to link with family members, friends, classmates and colleagues. Social sites allow for the creation of groups. This is based on the likeness of ideas and goals.

User Image sharing social site maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users unknowingly shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, Adaptive Privacy Policy Prediction (A3P)[6] system is proposed to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of user's privacy preferences. We propose a two-level framework which according to the user's available history on the site

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

determines the best available privacy policy for the user's images being uploaded. Our solution relies on an image classification framework for image categories which may be associated with similar policies and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. The generated policies will follow the evolution of users' privacy attitude.

Adaptive Privacy Policy Prediction (A3P)[6] system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P[6] system handles user uploaded images, the impact of social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. The impact of social environment and personal characteristics, social context of users, such as their profile information and relationships with others may provide useful information regarding user's privacy preferences. A3P[6] system is comprised of two main building blocks A3P-Social and A3P-Core. The A3P-core focuses on analyzing each individual user's own images and metadata, A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. A3P-core: (i) Image classification and (ii) Adaptive policy prediction. User images are first classified based on content and metadata. Privacy policies of each category of images are analyzed for the policy prediction. Content-based classification algorithm compares image signatures defined based on quantified and sanitized version of Hear wavelet transformation. Metadata-based classification groups images into subcategories under aforementioned baseline categories. A3P-social multi-criteria inference mechanism that generates representative policies by leveraging key information related to the user's social context. Adaptive Privacy Policy Prediction (A3P) system that helps users automates the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold start, leveraging social context information

The impact of social sites and personal characteristics: A social sites is an online platform that is used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. The variety of stand-alone and built-in social networking services currently available in the online space introduces challenges of definition.

. Social networking sites allow users to share ideas, digital photos and videos, posts, and inform others about online or real world activities and events with people in their network. While in-person social networking, such as gathering in a village market to talk about events has existed since the earliest developments of towns, the Web enables people to connect with others who live in different locations, ranging from across a city to across the world.

Image's content and metadata: Image files can contain information about the content of the images, the image rasters, and image metadata. In general, similar images often incur similar privacy preferen-ces, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos. He may upload some other photos of landscapes which he took as a hobby and for these photos, he may set privacy preference allowing anyone to view and comment the photos.

2. RELATED WORK

A. Acquisti and R. Gross [1] proposed that online social networks such as Friendster, MySpace, or the Facebook have experienced exponential growth in membership in recent years. These networks offer attractive means for interaction and communication, but also raise privacy and security concerns. In this study we survey a representative sample of the members of the Facebook (a social network for colleges and high schools) at a US academic institution, and compare the survey data to information retrieved from the network itself. We look for underlying demographic or behavioral differences between the communities of the network's members and non-members; we analyze the impact of privacy concerns on members' behavior; we compare members' stated attitudes with actual behavior; and we document the changes in behavior subsequent to privacy-related information exposure. We find that an individual's privacy concerns are only a weak predictor of his membership to the network. Also privacy concerned individuals join the network and reveal great amounts of personal information. Some manage their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, we also find evidence of members' misconceptions about the online community's actual size and composition, and about the visibility of members' profiles.

S.Ahern, D. Eckles et al [2] described that sharing personal media online becomes easier and widely spread, new privacy concerns emerge – especially when the persistent nature of the media and associated context reveals details about the physical and social context in which the media items were created. In a first-of-its-kind study, we use context-aware camerephone devices to examine privacy decisions in mobile and online photo sharing. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, we identify relationships between location of photo capture and photo privacy settings. Our data analysis leads to further questions which we investigate through a set of interviews with 15 users. The interviews reveal common themes in privacy considerations: security, social disclosure, identity and convenience. Finally, we highlight several implications and opportunities for design of media sharing applications, including using past privacy patterns to prevent oversights and errors.

J. Bonneau, J. Anderson et al [3] described about creating privacy controls for social networks that are both expressive and usable is a major challenge. Lack of user understanding of privacy settings can lead to unwanted disclosure of private information and, in some cases, to material harm. We propose a new paradigm which allows users to easily choose "suites" of privacy settings which have been specified by friends or trusted experts, only modifying them if they wish. Given that most users currently stick with their default, operator-chosen settings, such a system could dramatically increase the privacy protection that most users experience with minimal time investment.

Ricardo da Silva Torres et al [4] Advances in data storage and image acquisition technologies have enabled the creation of large image datasets. In this scenario, it is necessary to develop appropriate information systems to efficiently manage these collections. The commonest approaches use the so-called Content-Based Image Retrieval (CBIR) systems. Basically, these systems try to retrieve images similar to a user-defined specification or pattern (e.g., shape sketch, image example). Their goal is to support image retrieval based on content properties (e.g., shape, color, texture), usually encoded into feature vectors. One of the main advantages of the CBIR approach is the possibility of an automatic retrieval process, instead of the traditional keyword-based approach, which usually requires very laborious and time-consuming previous annotation of database images. The CBIR technology has been used in several applications such as fingerprint identification, biodiversity information systems, digital libraries, crime prevention, medicine, historical research, among others. This paper aims to introduce the probe ms and challenges concerned with the creation of CBIR systems, to describe the existing solutions and applications, and to present the state of the art of the existing research in this area.

Alexandru Lucian Ginsca et al [5] The availability of large annotated visual resources, such as ImageNet, recently led to important advances in image mining tasks. However, the manual annotation of such resources is cumbersome. Exploiting Web datasets as a substitute or complement is an interesting but challenging alternative. The main problems to solve are the choice of the initial dataset and the noisy character of Web text-image associations. This article presents an approach which rst leverages Flickr groups to automatically build a comprehensive visual resource and then exploits it for

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

image retrieval. Flickr groups are an interesting candidate dataset because they cover a wide range of user interests. To reduce initial noise, we introduce innovative and scalable image reranking methods. Then, we learn individual visual models for 38,500 groups using a low-level image representation. We exploit o -the-shelf linear models to ensure scalability of the learning and prediction steps. Finally, Semfeat image descriptions are obtained by concatenating prediction scores of individual models and by retaining only the most salient responses. To provide a comparison with a manually created resource, a similar pipeline is applied to ImageNet. Experimental validation is conducted on the ImageCLEF Wikipedia Retrieval 2010 benchmark, showing competitive results that demonstrate the validity of our approach.

Anna Cinzia Squicciarini et al [6] describes that with the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. We propose a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.

3 SYSTEM OVERVIEW

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behaviour. If one of the following two cases is verified true, A3P-core will invoke A3P-social: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc). In above cases, it would be beneficial to report to the user the latest privacy practice of social communities that have similar background as the user. The A3P-social groups users into social communities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction.

4 A3P CORE

The A3P-core focuses on analyzing each individual user's own images and metadata. There are two major components in A3P-core: (i) Image classification and (ii) Adaptive policy prediction. For each user, his/her images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction.

4.1 Image Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have meta-data will be grouped only by content. Such a hierarchical classification gives a higher priority to image

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

content and minimizes the influence of missing tags. Note that it is pos-sible that some images are included in multiple categories as long as they contain the typical content features or meta-data of those categories.

4.1.1 Content-Based Classification

Content-based classification is based on an efficient and yet accurate image similarity approach. Classification algorithm compares image signatures defined based on quantified and sanitized version of Hear wavelet transformation. The Image encodes frequency and spatial information related to image color, size, and texture. The small number of coefficients is selected to form the signature of the image.

4.1.2 Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. Extract keywords from the metadata associated with an image metadata vector frequency find a subcategory that an image belongs to. This is an incremental procedure. The privacy approach with in same category of the new image user defines a policy same category of the new image, conduct association rule mining on the subject component of polices.

5 A3P-SOCIAL

The image data collection, To image predict policies and compare it with a base-line algorithm which does not consider social contexts but bases recommendation only on social groups that have similar privacy strictness of images information. Using the base-line approach, we note that regardless of the individual privacy inclination of the users, the best accuracy is achieved in case of explicit images and images dominated by the appearance Image. Users maintain more consistent policies, and our algorithm is able to teach them effectively. Images searching for content based and image based the result found for each image privacy policy set of user privacy in sharing site.

6. PROPOSED WORK

Even though many privacy policies are set for images, sometimes the images are exposed through search engines. To overcome the disadvantage of existing system, a haar discrete wavelet transformation algorithm which is a type of DWT algorithm is used to create a signature for all newly uploaded images to the site. The signature is created by using the image features such as size, color and texture to calculate the haar value for all images. Through this signature images can be restricted from exposing through search engine.

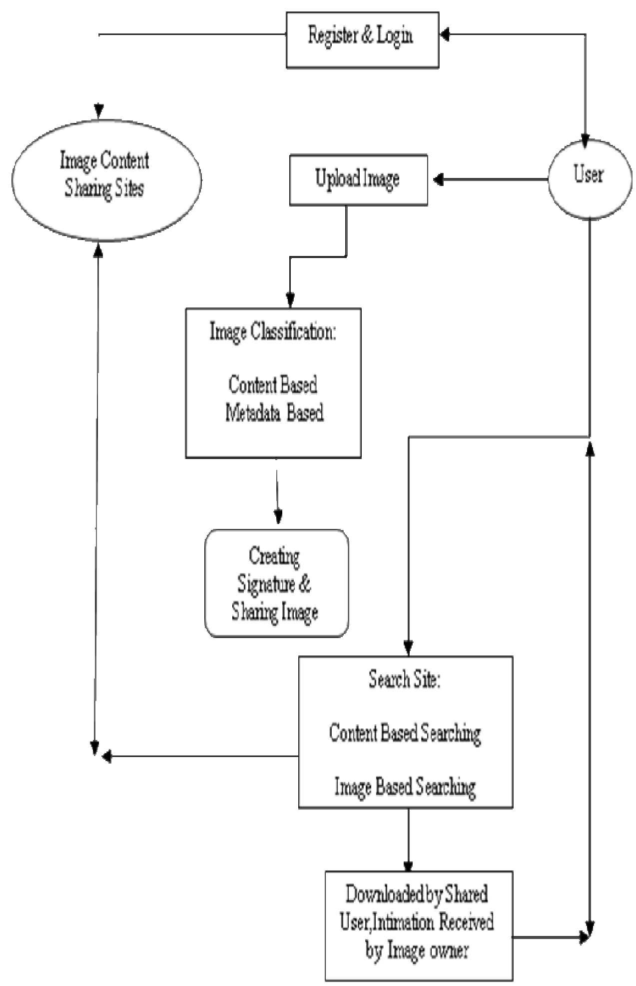

Fig.1. System Architecture

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

6.1 Signature Creation

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere e. g. the dilation equation

$$\phi(x) = \sum_{k=-\infty}^{\infty} a_k \phi(Sx - k).$$

where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be orthogonal to its integer translates e. g.

$$\int_{-\infty}^{\infty} \phi(x)\phi(x+l)dx = \delta_{0,l}$$

After introducing some more conditions (as the restrictions above does not produce unique solution) we can obtain results of all this equations, e. g. finite set of coefficients a and k which define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as

$$\psi(x) = \sum_{k=-\infty}^{\infty} (-1)^k a_{N-1-k} \psi(2x - k)$$

where N is an even integer. The set of wavelets than forms an orthonormal basis which we use to decompose signal. Note that usually only few of the coefficients a_k are non zero which simplifies the calculations.

6.2 Texture Algorithm

Texture synthesis is an alternative way to create textures. Because synthetic textures can be made of any size, visual repetition is avoided. Texture synthesis can also produce tolerable images by properly handling the boundary conditions. Potential applications of texture synthesis are also broad; some examples are image de-noising, occlusion fill-in, and compression.

The problem of texture synthesis can be stated as follows: Given a texture sample, synthesize a new texture that, when perceived by a human observer, appears to be generated by the same underlying stochastic process. An example is shown in the above figure. Our goal is to develop a new texture synthesis algorithm that is efficient, general, user-friendly, and able to produce high quality textures. In addition, we would like to extend the horizon of texture synthesis by exploring a variety of new applications based on our algorithm.

7 CONCLUSION

Once the signature is created for the image, it can be shared by setting our own policies. Only the shared persons are able to see the images. The system is also employed with some additional features such as to know the person who views the shared images and also to know the person who downloaded the shared images.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[2] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

[3] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[4 Ricardo da Silva Torres, Alexandre Xavier Falcão "Content-Based Image Retrieval: Theory and Applications".

[5] Alexandru Lucian Ginsca, Adrian Popescu, Herv_e Le Borgne, Nicolas Ballas,
Phong Vo, Ioannis Kanello" Large-scale Image Mining with Flickr Groups".

[6] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites

[7] J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., 2009, pp.249–254.

[8] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.

[9] X. Su and T. M. Khoshgoftaar, "A survey of collaborative filtering techniques," Adv. Artif. Intell., vol. 2009, p. 4, 2009.

[10] X. Sun, H. Yao, R. Ji, and S. Liu, "Photo assessment based on computational visual attention model," in Proc. 17th ACM Int. Conf. Multimedia, 2009, pp. 541–544. [Online]. Available: http:// doi.acm.org/10.1145/1631272.1631351

[11] H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev, "Multimedia semantics: Interactions between content and community," Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.

[12] A. Vailaya, A. Jain, and H. J. Zhang, (1998). On image classifica- tion: City images vs. landscapes. Pattern Recog. [Online]. 31(12), pp. 1921–1935. Available: http://www.sciencedirect.com/ science/article/pii/S003132039800079X

[13] R. A. Wagner and M. J. Fischer, "The string-to-string correction problem," J. ACM, vol. 21, no. 1, pp. 168–173, 1974.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your ulti-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

[14] Wordnet - A lexical database for the English language. [Online]. Available: http://wordnet.princeton.edu/

[15] C.-H. Yeh, Y.-C. Ho, B. A. Barsky, and M. Ouhyoung, "Personalized photograph ranking and selection system," in Proc. Int. Conf. Multimedia, 2010, pp. 211–220. [Online]. Available: http://doi.acm.org/10.1145/1873951.1873963

[16] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[17] J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.

[18] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.

.